REMARKS

With this Response, no claims are amended, added, or canceled. Therefore, claims 1-38 are pending.

MATTERS RESOLVED

Applicants kindly acknowledge that the previous claim objections, claim rejections under 35 U.S.C. § 112, and the claim rejections under 35 U.S.C. § 101 have been withdrawn.

CLAIM REJECTIONS - 35 U.S.C. § 102

The rejection of claims 1-38 under 35 U.S.C. § 102 was maintained in the Final Office Action. More particularly, these claims were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2004/0039924 of Baldwin et al. (hereinafter "Baldwin"). Applicants maintain that these claims are not anticipated by the cited reference for at least the following reasons, including a reply to the Response to Arguments section of the Final Office Action.

Applicants' previous Response focused on the claim language directed to a storage not directly accessible to the host **processor** on the client (claims 1 and 29), a network link transparent to the host processor and the OS (claim 11), and a communication channel accessible to the chipset and not the host platform (claim 22). In summary, Applicants submit that Baldwin teaches away from such claim limitations, has storage only directly accessible to the host processor, and requires the use of the host processor in its operations. The Final Office Action asserts at page 3 that Baldwin's CryptoEngine

> performs in a restricted mode that is only accessible during normal operation by transferring control from a normal mode of the processor to a restricted mode of the processor via CryptoGate. The examiner notes a 'restricted mode' is not directly accessible to a host processor on a client.

Applicants note that the argument in the Final Office Action is self-conflicting. The Final Office Action states that the "restricted mode" is not directly accessible to the host processor, and yet also acknowledges that it is the very same host processor that executes in the restricted mode. Applicants request clarification on how a processor becomes a different processor when operating in a restricted mode. Applicants' claims recite a storage not accessible to a processor, not a storage that can only be accessed by a processor in a special state. Note that the processor

accessing the storage "in a restricted mode" means the storage is accessible to the processor, and **does not** mean that the storage is **not accessible** to the processor. Applicants respectfully submit that whether the host processor accesses the storage disclosed in Baldwin in "normal mode" or "restricted mode," **the host processor still directly accesses the storage**, and thus in contrast to what is claimed, the storage cannot be a storage not directly accessible to the host processor.

Furthermore, Applicants suspect that the following question is answered with the argument above, but Applicants submit that the statement in the Office Action that "a 'restricted mode' is not directly accessible to a host processor on a client" does not appear to be a logical statement. As noted above, it is the host processor that operates in the "restricted mode," so the restricted mode can only be accessible to the host processor, given it is the host processor on the client that operates in the restricted mode. If the Office Action intended to suggest something other than asserting that the processor does not have access to itself, it was not clear from the Office Action.

To reiterate what Applicants previously submitted, Baldwin fails to disclose or suggest the invention as recited in the independent claims, and in fact **teaches away** from what is claimed. As explicitly stated in Baldwin's "Objectives of Present Invention" section, paragraphs [0009] to [0013], the teachings or Baldwin are directed to providing "a system that permits for computer device authentication that requires exactly no more hardware than in found in a commodity-class commercial personal computer." Although Applicants appreciate that such a term may be considered vague at least as far as the hardware found in a commodity-class commercial personal computer will change over time, Baldwin describes "a minimum of hardware" as being the intended implementation platform for its systems. See also paragraph [0015]. The reference goes to great detail to describe a system in which a reboot sequence and an SMM (system management mode) are used to provide secure operations. See "Key aspects of the present invention" as set forth in paragraphs [0017] to [0029]. Baldwin explicitly limits its application to the **SMM implementation** described. As is understood by one of skill in the art, although SMM may be outside the context of a **host operating system**, SMM executes **on the host processor** of the system. Thus, executing in SMM explicitly **requires** that the host processor have access to all of the resources used to provide the security. Thus, even assuming independence from the host OS, SMM and the solutions presented in Baldwin prevent independence from the host processor. More particularly, one of skill in the art would understand

that Baldwin explicitly requires the host hardware platform including the host processor to have access to the cryptographic keys and the secure communication channels. Without such access, Baldwin's described system **could not be implemented in the manner described**. That is, SMM as described only works when the host processor has access to the resources, such as storage in which the keys are stored. Such a requirement is at least one reason Baldwin asserts in paragraph [0015] to suggest that allowing the host hardware to have such access provides only a minimal security risk. That security risk described was in reference to the fact that the processor, in the secure mode, was accessing the secure data. Such a statement would be meaningless if the storage was actually inaccessible to the processor, because then the security risk discussed would not exist. Thus, the teachings of Baldwin are directly contrary to what is claimed, and the reference is inapplicable in rejecting Applicants' claims.

In direct contrast to what is discussed in Baldwin, Applicants' claims all recite features directed to something inaccessible, transparent, or otherwise independent from the host processor. See above: "a storage" in claims 1 and 29, "a network link" in claim 11, and "a communication channel" in claim 22. Thus, Baldwin is incapable of disclosing or suggesting at least one feature of the claimed invention, and so fails to support an anticipation rejection of the independent claims as per MPEP § 2131.

The remaining claims depend directly or indirectly from the independent claims, and are thus necessarily not anticipated by the cited reference for at least the reasons set forth above.

CONCLUSION

For at least the foregoing reasons, Applicants submit that the rejections have been overcome. Therefore, all pending claims are in condition for allowance, and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: February 21, 2008

/Vincent H. Anderson/
Vincent H. Anderson
Reg. No. 54,962
Attorney for Applicant

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below.

Date: 2/21/2008 /Katherine Jennings/
Katherine Jennings